# Wireless Site Survey and Placement Guide for SOHO TZW

*Prepared by SonicWALL, Inc.*
04/15/2003

**Introduction**
Unlike other types of networking devices, the proper installation and placement of the SonicWALL SOHO TZW is crucial to its successful operation. This technote will discuss the factors that can be used to determine what 'proper placement' will be for your environment.

Ideally, the SOHO TZW will be placed in an indoor area where the largest number of wireless users have the best "point a to point b" path to it, with the fewest number of environmental obstructions. In most buildings, the best location for a SOHO TZW would be centrally mounting the device on the ceiling, with both antennas pointed straight down towards the users. Unfortunately, since power and ethernet cabling must also be run to the SOHO TZW, ceiling mounting is sometimes not possible. An alternative is centrally mounting the SOHO TZW on a raised pedestal such that the two antennas are not blocked by any environmental factors (walls, cubicle dividers, steel I-beams, etc). Indoors, you can expect the signal to reach from 100 to 150 feet at 11Mbps using the 'High' power setting, but this is entirely dependent upon building construction, environmental factors, and placement issues of both the SOHO TZW itself and the antennas of the wireless clients. You will also need to consider the composition of flooring material itself when placing SOHO TZW's above and below each other on different floors.

Failure to properly install & orient the SOHO TZW will result in most of your wireless users being unable to connect, constant retransmission errors, and low throughput for the few users that are even able to associate with the SOHO TZW. Luckily, doing some advance planning before you install your SOHO TZW should prevent this from occurring.

**The Enemies of 802.11b Wireless**
Distance -- aka 'path loss'. High frequency signals, such as the ones used for 802.11b wireless (2.4Ghz), are especially sensitive to the distance between the radio and the wireless client. In order to compensate for distance, wireless clients will lower their speed in an attempt to maintain connection. As an 802.11b wireless card moves farther away from the SOHO TZW, the path loss increases, and will cause the signal-to-noise ratio to decrease to the point where the data signal is indistinguishable from the noise. In the best circumstances, the SOHO TZW will have an effective indoors range of 100-150 feet at 11Mbps. The farther away the wireless client is from the SOHO TZW, the more likely it will have problems connecting with it, and the slower the connection speed will be. When conducting your site walk (see below), be sure to note the distances from your wireless users to the planned install points.

Active Interference -- Because 802.11b wireless uses carrier sensing medium access protocols, a wireless station will not transmit when it senses other "stations" transmitting. If the interfering signal falls within the same frequency range of the station, then the interfering signal will appear legitimate and block the radio from transmitting. The interfering signal can also strike a packet in transit, resulting in errors, retransmissions, and corresponding delays. The 802.11b ISM (Industrial, Scientific, Medical) band is subject to interference from multiple external sources – 2.4Ghz cordless phones, X10 surveillance gear, baby monitors, wireless medical equipment, microwaves, and Bluetooth devices (especially these since they hop frequencies 1600 times faster than 802.11b devices). It may be necessary to move these devices away from the SOHO TZW and its wireless clients to minimize the potential for signal interference.

Passive Interference -- aka 'attenuation'. The 802.11b signaling can be significantly impeded by environmental factors. Obstructions such as metal walls, I-beams, concrete, marble, or brick will cause a high degree of signal loss. Obstructions such as water, people, or trees will cause a medium degree of signal loss. Obstructions such as wood, plaster, cubicle partitions, or glass may cause a low degree of signal loss. When conducting your site walk (see below), it will be important to mark these sorts of obstructions on your site chart.

Signal reflection -- aka 'multipath propagation'. Transmitted radio signals can be corrupted by reflected/bounce signals. These signals can be reflected by walls, furniture, machinery, etc. The more reflective surfaces there are, the more multipathing and ISI (Inter-Symbol Interference) occurs, forcing retransmissions, and slowing the effective overall data rate. Unfortunately, 802.11b is very susceptible to multipath propagation because of its wide channel, continuous transmission characteristics. The most common solution to this problem is antenna diversity – using more than one antenna and adaptively selecting the best one. The SOHO TZW uses this method to deal with signal reflection.

**Antenna Orientation**

The SOHO TZW ships with two 5dBi omnidirectional antennas, also known as 'rubber ducky' antennas, both of which can be oriented in any direction. These antennas, combined with the radio signal strength, are what give the SOHO TZW its effective indoor range of 100-150 feet at 11Mbps. Although it is possible to detach the 'rubber ducky' antennas from the SOHO TZW, SonicWALL does not currently sell, recommend, or support external antennas. Please note that the FCC regulates power output of 802.11b wireless devices to no more than 30dB; attaching high-gain antennas to the SOHO TZW may violate FCC regulations regarding power output.

The name 'omnidirectional antenna' pretty much gives away how the signal emanates. Some people like to refer to this type of signal as donut-shaped, but it's easier to think of an omnidirectional antenna as behaving like a lantern (see below). As with a lantern, there are 'dead spots' directly above and below the antenna. Your users need to be "in the light". You will need to consider this characteristic when orienting the antennas of the SOHO TZW – do not place wireless users in these 'dead spots'. If you are unable to position the SOHO TZW or orient its antennas properly in order to avoid this, it may be necessary to instead move the wireless user into the coverage area.

***with omnidirectional antennas . . .***

It is sometimes necessary to outfit distant wireless users, or those users whose signal is reduced by environmental factors with a more appropriate wireless card. Many wireless cards currently on the market are not especially powerful, or do not have good signal recieve sensitivity, which means that they will only function well if they are relatively close to the SOHO TZW. Companies such as Senao market high-power cards that also have exceptional signal receive sensitivity, which is a critical and often overlooked factor. When dealing with signal problems, it is sometimes useful to imagine that the SOHO TZW and wireless user are like two people standing at the opposite ends of a football field. Both people must have a strong voice and good ears to communicate with each other all the way across the field. Possessing only one of these qualities will make communication difficult – you have to have both. Given this, be sure to choose a wireless card that has high power and good signal receive sensitivity in order to alleviate connectivity and throughput issues. Look for wireless cards that operate at 100mw to 200mW, and cards with receive sensitivity between –85dB to –95dB.

Of course, it may be a better solution simply to place another SOHO TZW closer to these users, rather than trying to shout across the distance or blast through thick walls and floors with a high-powered signal. It may also turn out that placing additional SOHO TZW's throughout your site is less expensive than replacing everyone's wireless card with stronger models.

**Power, Channel, and Signal**

There are four adjustable settings that control the signal strength of the SOHO TZW's wireless radio: High, Medium, Low, and Lowest. Please note that merely increasing the power setting in the SOHO TZW may not necessarily solve connectivity problems with wireless clients. Boosting the signal in the SOHO TZW only increases the SOHO TZW's signal strength – it does not make the SOHO TZW any more sensitive to weak signals emanating from the wireless clients themselves. As noted above, wireless clients having trouble connecting to the SOHO TZW because of distance issues or environmental issues may need to replace their wireless cards with more powerful and sensitive models.

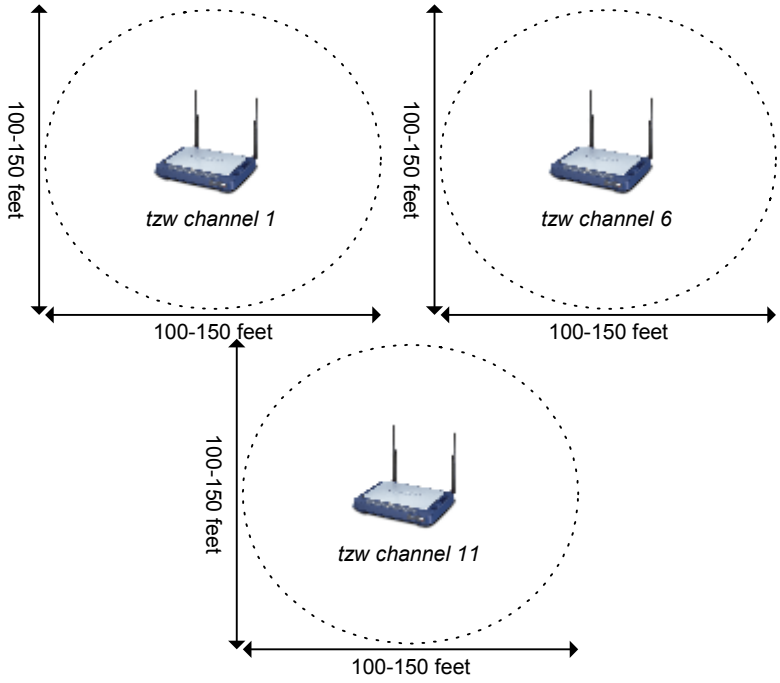
The lower you adjust the radio's power setting, the shorter the coverage distance will be. Each reduction in setting will result in roughly half the distance of the previous setting. For example: using the 'High' setting at 11Mbps will result in a coverage distance of roughly 100-150 feet. Reducing the setting to 'Medium' will result in a coverage distance of roughly 50-75 feet, and so on. This can be especially useful when you wish to prevent signal bleed into unwanted areas, such as out into public areas (i.e. parking lots and sidewalks), or into adjacent buildings that are occupied by other companies. Conversely, adjusting the speed of the management frames to a higher setting will shorten the distance it will travel, since high speed signals do not travel as far as lower-speed signals. Adjusting these settings also have the side effect of making you a 'good neighbor' – your SOHO TZW's signal will be less likely to interfere with other people's remote access points not in your control.

If you only have one SOHO TZW, you may set it to any channel you wish, within the rules of your geographic region. However, if you have more than one SOHO TZW within several hundred feet of each other, signal overlap interference is likely to occur unless the access point channels are spaced appropriately. Due to the signaling mechanism in 802.11b, there is significant overlap across the eleven available channels for North America. For instance, the signal for channel one overlaps the next four channels (two through five), and the signal for channel six overlaps the next four channels (seven through ten). This means that access points within range of one another must be set to channels that do not overlap. If you were to have two access points, you could set them to 1/6, 2/7, 3/8, 4/9, 5/10, or 6/11. If you were to have three access points, you could only set them to 1/6/11.

Rules of thumb:

- Plan for 200-foot buffer between SOHO TZW's operating on the same channel
- Plan for three SOHO TZW's per five-story building to avoid signal degradation
- Conduct frequent scans for unknown, or 'rogue', access points
- Be a 'good neighbor' and adjust power settings accordingly
- 20-25 unique wireless users max per SOHO TZW device – less if they are "power users"

**Remember to think in 3D when placing multiple SOHO TZW Devices…**




The triangular placement pattern above can be repeated up/down or left/right, as it will use at least one of the SOHO TZW's as a buffer between potentially overlapping channels.

SonicWALL does not sell, recommend, or support external 802.11b signal amplifiers. Connecting an external amplifier to the SOHO TZW may void the warranty of the product, as well as potentially violate FCC regulations for output power. In short, do **NOT** connect an external amplifier to the SOHO TZW.

**Site Survey**

Before you do your site walk, you will need to obtain blueprints or floor plans for the building. If these are not available, you can always draw your own – but be sure to leave lots of room for notation. This 'site map' is what you will use to decide upon the best location to install the SOHO TZW.

Plan on taking up to a full day to complete this task, as it may take a lot of time to walk through the entire site with the survey tools, take the necessary readings, and document them onto the site map. If you have already chosen potential installation points, note them first on the site map. From these potential points, map all distances, signal readings, and speeds seen from each location throughout the site. Also, make note of any external factors that may affect signal reception on the site map, as described in the 'Enemies of 802.11b Wireless' section. Be sure to highlight any 'dead areas' you find on the site map—these areas may be candidates for high-power wireless cards, or dedicated SOHO TZW devices.

You can use the SOHO TZW during the site survey process as a means of measuring signal strength. Out of the box, the SOHO TZW will broadcast on channel 11 with a SSID of 'sonicwall' at full signal strength, so there is no need to configure anything in order to do the site survey. Place the SOHO TZW at the potential install points, power it up, and you should be ready to go. You can move the SOHO TZW around as needed during the day since it needs no configuration and is not yet in use.

**Wireless Site Survey and Placement Guide for SOHO TZW**

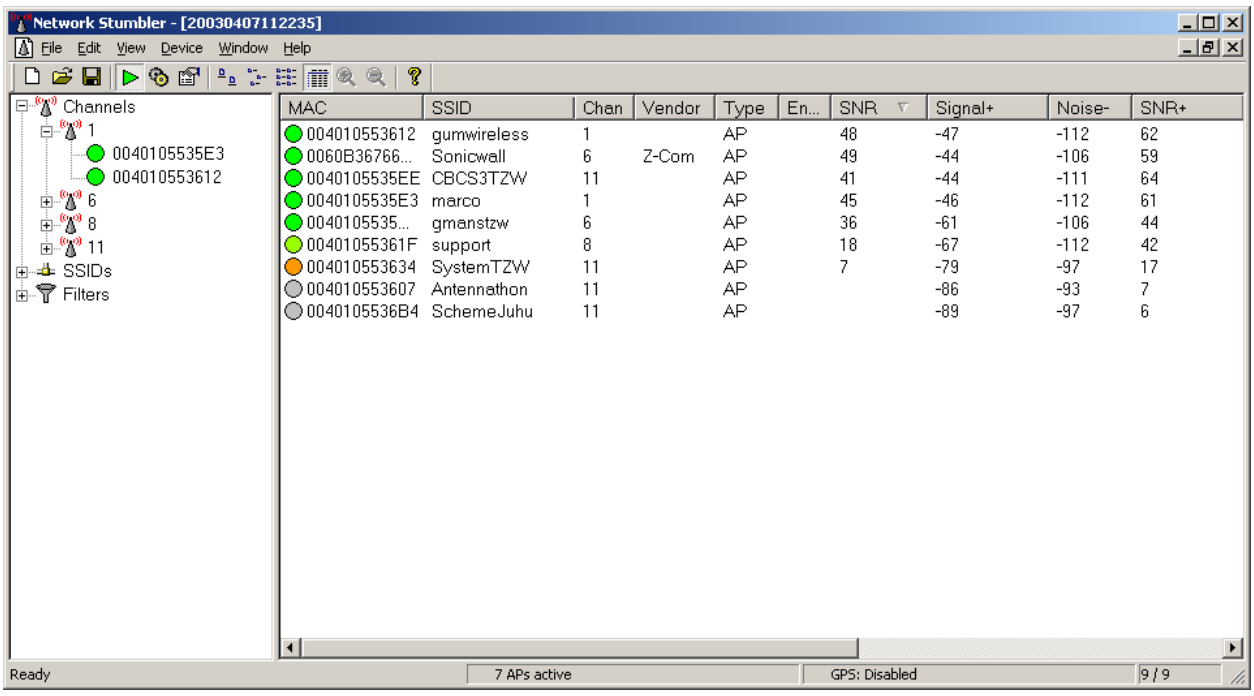
There are several tools for performing site surveys available to you. Some wireless card manufacturers offer simple survey tools as a part of the card's diagnostic software. Other third-party companies offer specialized software packages to perform site surveys, such as WildPackets' "AiroPeek", or AirMagnets' "AirMagnet Laptop Pro", but these tools can cost thousands of dollars. For this technote, we will be using a tool called "Netstumbler", which is a free Windows-based software package available at http://www.stumbler.net. It is compatible with a number of inexpensive wireless cards currently on the market. For this paper, we ran Netstumbler on a Windows XP laptop using a Proxim 'Orinoco' wireless PC card.

## Using Netstumbler

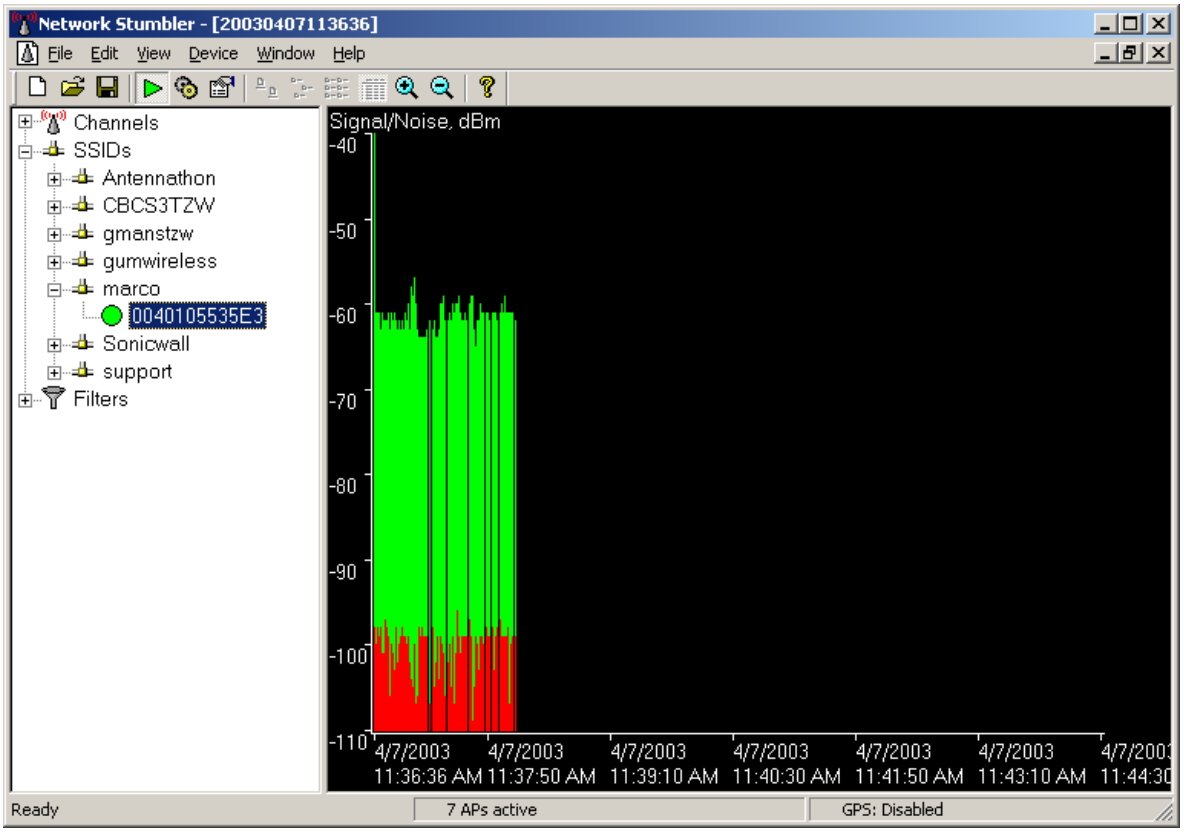
At its core, Netstumbler is a program that takes control of your wireless card and forces it to scan all available wireless channels, broadcasting what's known as a Probe Request management frame on all channels. These Probe Requests attempt to force all wireless access points to respond with a Probe Response management frame, which contains all the necessary data for a wireless card to associate with the access point. Netstumbler uses the responses to build a database of access points it has seen while the program has been running, and plots a running graph of the signal strengths of each of these access points. It is easy to use and extremely effective at mapping access points; unfortunately, it is for these very reasons that many wardrivers use it to find unprotected access points. There are methods to hide your SOHO TZW from Netstumbler, which we will discuss later on in this paper.

We'll be using Netstumbler to determine three factors: the signal strength of various points around your site, potential active signal interference, and signal bleed into unwanted areas. Our SOHO TZW used for this test has a SSID of "marco" and is broadcasting on Channel 1. We've placed it in the center of the building, sitting on top of a desk.

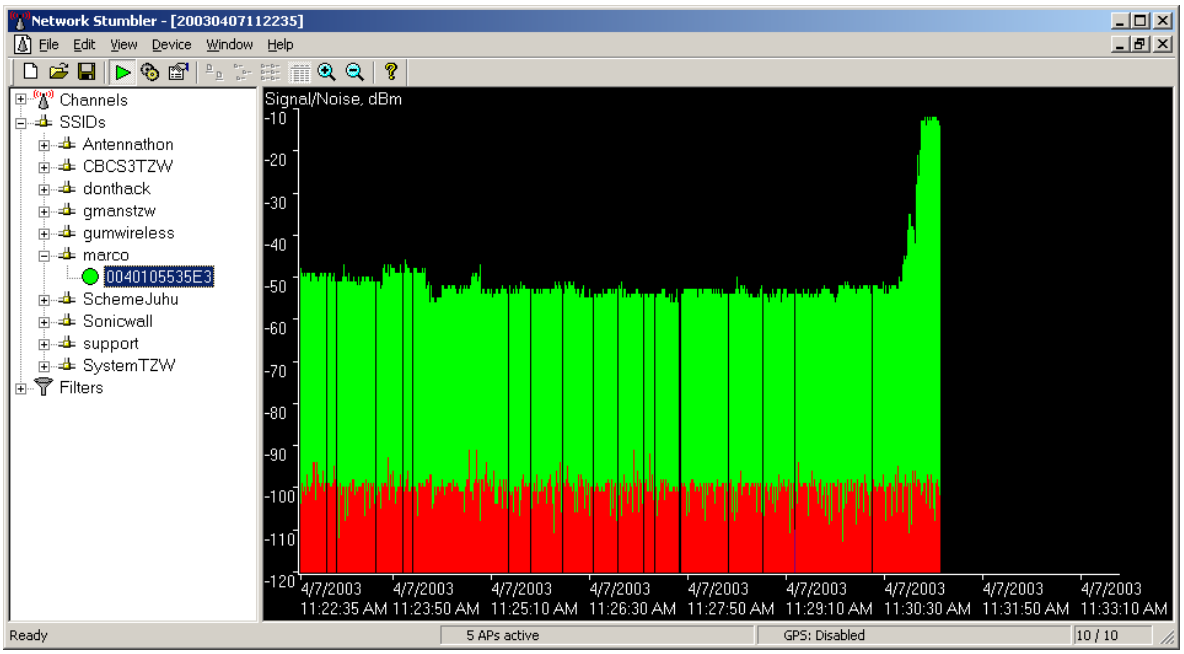
Below is a screenshot of Netstumbler running during our initial sitewalk. As you can see, there are a number of access points already active, in addition to the SOHO TZW we placed at the planned install point. You can sort the results by any of the columns – ours is sorted by SNR in descending order of the strongest to weakest signal our laptop sees. Already, we can see that there may be significant problems with channel overlap at our site. Final placement of our SOHO TZW will have to factor these other access points.



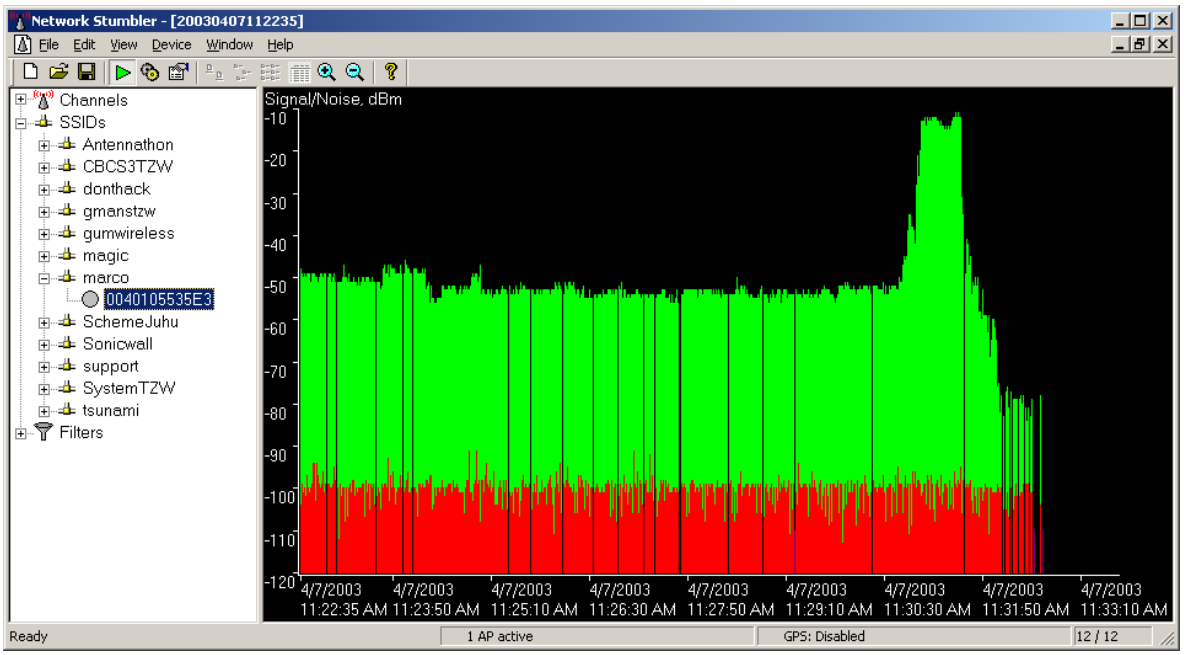
Below is a screenshot of the Signal/Noise real-time graph taken at 40 feet from the SOHO TZW, through two drywalls. We can see that the signal, despite the distance and the environmental factors, is still usable.



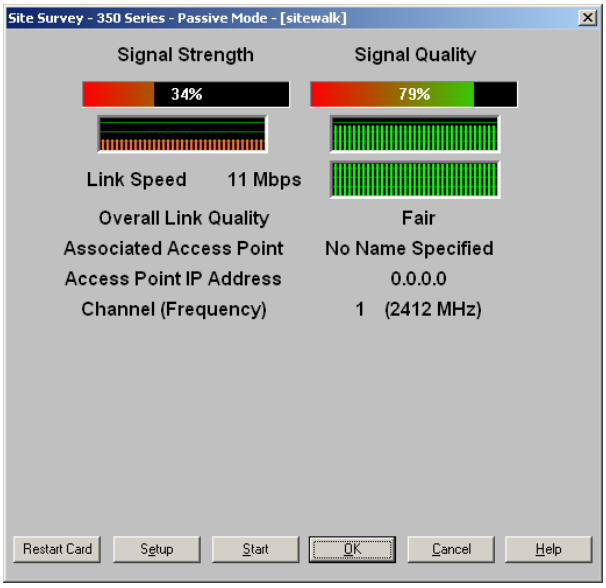

As we get closer to the SOHO TZW, the signal increases dramatically. This is from 15 feet away.



We then walked out into the middle of the parking lot while Netstumbler was still running – about 150 feet from where we placed the SOHO TZW. While the signal has decreased a significant amount, it is still detectable, and potentially usable. A more powerful card with good receive sensitivity (and perhaps an external directional antenna) could latch onto this signal and use it. Since we're in our parking lot, this is clearly not a good thing. This tells us that we should probably adjust the power in the SOHO TZW and take further readings out here.




Just to test this theory, we replaced the Proxim Orinoco wireless card with a Cisco 350 wireless card, which has extremely good receive sensitivity, and can be cranked up to 100mW power output. Sure enough, we were able to stand out in the parking lot, successfully attach to the SOHO TZW, and surf the web from there. The screenshot below shows the signal readings from the Cisco card while standing in parking lot. So we'll definitely be tuning the power output down, as well as activating some security features to be safe.



**Security Considerations**

The SOHO TZW has a number of 'deflective' security features that can be enabled to deter most attempts to gain unauthorized access to the SOHO TZW. The term 'deflective' is used because these methods do not truly ensure security – they just make it extremely difficult for anyone trying to compromise the SOHO TZW. The only true way to provide wireless security is enforcing WiFiSec usage across all wireless clients, but the methods below are better than nothing:

- You can remove the SSID from management beacon frames that the SOHO TZW sends out. This forces all wireless clients to manually enter the SOHO TZW's SSID into the settings before it can successfully connect.

- You can stop the SOHO TZW from responding to management probe request frames using a null SSID from wireless clients. Many wireless sniffing & cracking toolkits available on the Internet allow the wireless card to send out management probe request frames, which seek to force the access point (i.e. the SOHO TZW) to respond with its connection details. Enabling this feature causes the SOHO TZW to ignore and not respond to these attempts.

- You can use MAC filter lists on the SOHO TZW. By enabling this feature, the SOHO TZW will not allow wireless clients to associate unless the MAC address of that wireless client has been added to its internal 'allow' list.

- You can enforce the use of WEP on the SOHO TZW. By enabling this feature, all wireless clients will need to manually enter one of the four WEP keys configured on the SOHO TZW.

- You can enforce the use of Wireless Guest Services (WGS). By enabling this feature, all wireless clients must authenticate themselves to the SOHO TZW via HTTP before they are allowed access to resources on the WAN. The user and password database can either be stored onboard the SOHO TZW, or the SOHO TZW can authenticate users from external RADIUS servers.

- You can disable DHCP services on the WLAN interface. This will require all of your wireless clients to input the correct IP information manually, but it will prevent unwanted wireless clients from obtaining DHCP lease information from the SOHO TZW. Alternately, you can configure DHCP services to only hand out leases to specific MAC addresses.

- As noted previously, you can adjust the power and management frame settings. Tuning these settings properly will prevent your wireless signal from bleeding into unwanted areas (out into public areas, into adjacent buildings occupied by other companies, neighbors' houses, etc). Wardrivers often look for public spots into which a usable signal has leaked, so take this into account when adjusting your SOHO TZW.